Uma solução IPSec para comunicações seguras Anycast em redes IPv6

João Veiga, António Costa e Alexandre Santos, *Centro Algoritmi, Universidade do Minho*

***Abstract*—Neste artigo faz-se um levantamento do estado de arte das tecnologias Anycast e IPSec, testam-se as implementações existentes conjuntamente em cenários reais, e propõe-se uma solução capaz de permitir comunicações seguras entre um cliente e um conjunto de servidores com um mesmo endereço anycast. A solução proposta é totalmente baseada no IPSec e a sua utilização não implica nenhuma alteração às tecnologias usadas.**

***Index Terms*—IPv6, Anycast, IPSec, IKE, balanceamento de carga, segurança.**

I. Introdução

AO contrário do *Unicast* que possui uma filosofia de ”um para um”, e do *Multicast* que possui uma filosofia de “um para muitos” (*one to many*), o *Anycast* possui uma filosofia de “um para qualquer um” (*one to any*) [1]. Um pacote endereçado a um servidor *anycast*, é recebido pelo membro “mais próximo” do grupo *Anycast*, sendo que a proximidade é definida pelas métricas de rede implementadas pelos encaminhadores. Dois pacotes enviados pelo mesmo host para um endereço anycast, podem chegar a dois servidores anycast diferentes, dependendo da estabilidade da tabela de *routing*. Esta propriedade do anycast inviabiliza também a fragmentação de pacotes que possuam um endereço anycast como endereço de destino[2]. A utilização de ligações TCP torna-se também difícil devido a esta propriedade do anycast. O IPsec [3] consiste num conjunto de protocolos que visam proteger as comunicações das redes IP. O IPsec suporta autenticação ao nível da camada de rede, autenticação da origem dos dados, garante a integridade da informação, confidencialidade e ainda proteção contra ataques por repetição.

O objectivo deste trabalho consiste na análise do estado da arte das tecnologias IPSec e anycast, e no desenvolvimento duma solução que permita aliar o balanceamento de carga com a segurança: o balanceamento de carga será obtido utilizando o *anycast* e a segurança utilizando o IPsec. Posteriormente, pretende-se testar a solução num cenário prático e concluir sobre os seus resultados. A solução foi implementada utilizando o protocolo de *Internet* IPv6.

II. Análise de implementações anycast e IPSec

De modo a poder concluir sobre o estado actual e do suporte das tecnologias anycast e IPSec, planeou-se um cenário de teste de modo a testar as duas tecnologias.

Os aspectos observados foram: (1) tempo de recuperação em caso de falha de um servidor; (2) e em termos de balanceamento de carga. Os dois aspectos mencionados foram avaliados com o auxílio de um programa de testes desenvolvido em JAVA. Para a realização deste teste foram utilizados dois servidores para verificar se todos os pacotes TCP são enviados para o servidor correcto. De modo a avaliar o comportamento das comunicações *Anycast* em termos de tempo de recuperação em caso de falha de um servidor e ainda em termos de balanceamento de carga, foi desenvolvida a arquitectura de rede implementada no CORE, e foram também desenvolvidos dois programas em JAVA. O cliente cria a conexão TCP com o endereço *Anycast* do servidor e regista o tempo levado a efectuar e a receber as respostas. Foram efectuados os seguintes testes:

1 Tempo de recuperação em caso de falha, com os servidores à ”mesma distância”;
2 Tempo de recuperação em caso de falha, com os servidores a ”distâncias diferentes”;
3 Balanceamento de carga;

Na implementação dos testes, são aplicadas métricas que dependem do protocolo de encaminhamento utilizado para implementar as distâncias do cliente aos servidores.

Regista-se o tempo que levou a fazer os 100 pedidos, sendo os testes todos repetidos 15 vezes de modo a poderem ser obtidas conclusões a partir destes.

Ao implementar a arquitectura de rede com o protocolo de encaminhamento BGP, os servidores e o cliente foram colocados em AS diferentes. Para o protocolo BGP, apenas foram efectuados os testes 1 e 2, pelo facto do BGP não efectuar nenhum balanceamento de carga. Ao realizar o teste 1 e 2 observou-se que a diferença dos tempos apresentados nas duas situações não se revelaram estatisticamente relevantes.

Ao implementar a arquitectura de rede com o protocolo de encaminhamento OSPF, os servidores e o cliente foram colocados em áreas diferentes. Ao realizar o teste 1 e 2 observou-se que em caso de falha o cliente é reencaminhado para outro servidor, sendo que a diferença dos tempos apresentados nas duas situações não se revelaram estatisticamente relevantes. Relativamente ao teste 3 verificou-se que não é efectuado nenhum balanceamento de carga. No entanto, este facto pode dever-se à implementação do OSPFv3 utilizada pelo CORE, pois o *software* de *routing* do CORE não possui suporte *multipath routing*.

Após observar os tempos obtidos nos testes 1 e 2, foi possível observar a diferença de valores obtidos pelo BGP e OSPF, revelando-se este último mais rápido nas situações de falha.

É possível configurar o IPSec de dois modos: através da troca prévia de chaves secretas; e através da negociação dos parâmetros de segurança e das respectivas chaves secretas entre os dois extremos de uma conexão, IKE. A troca prévia

das chaves secretas introduz algumas reservas em termos de segurança, pois o modo como as chaves secretas são partilhadas nem sempre é devidamente controlado. O IKE é constituído por duas fases, a primeira de autenticação das extremidadas da conexão, e após esta ser concluída com sucesso a fase de negociação dos parâmetros de segurança. A negociação automática introduzida pelo IKE, torna-o num modo mais seguro de funcionamento quando comparado com a troca prévia das chaves secretas. Existem duas ferramentas de configuração do IPSec: o Racoon, e o Setkey. O Racoon permite a utilização do IKE, enquanto que o Setkey permite apenas o modo da troca prévia das chaves, através desta ferramenta é possível manipular directamente a SAD e a SPD.

Após testar os dois modos de funcionamento, IKE através do racoon e configuração manual através do setkey, verificou-se que não é possível, sem alterações, a utilização do IKE com o anycast. Após a análise do tráfego e dos resultados obtidos, observou-se que quando o cliente despoletava a negociação de SAs, para iniciar a negociação primeiro o cliente e o servidor *Anycast* necessitam de trocar mensagens(p.ex. *Neighbor solicitation*) através do protocolo ICMPv6; visto o servidor não responder a estes pacotes com o endereço *Anycast* no campo origem, mas sim com o unicast, é criado um problema de confiança resultando numa falha na fase de autenticação do IKE, não permitindo a criação das SAs. No entanto, manipulando a SAD e a SPD com o Setkey, utilizando chaves previamente partilhadas, verificou-se ser possível o estabelecimento de um canal IPSec entre o cliente e o servidor anycast.

III. Solução proposta

Nesta secção é apresentada a solução desenvolvida.

As tecnologias IPSec e *Anycast* não funcionam em simultâneo utilizando o IKE, devido aos problemas surgidos na fase de autenticação. Através da configuração manual é possível a utilização de ambas as tecnologias. No entanto este modo de configuração implica a troca prévia das chaves secretas, acrescentando aqui alguns problemas de segurança. Como tal, a solução proposta procura oferecer às comunicações entre clientes e serviços anycast segurança, usando IPSec, resolvendo os problemas da troca das chaves secretas e possibilitando assim a comunicação segura entre eles.

O objectivo da solução desenvolvida, é proteger a interação entre um cliente e um serviço *anycast*, através do IPSec. Funcionalmente a proposta está estruturada em 8 fases, que podem ser observadas na Figura 1. Correspondem a: (1) o cliente escolhe os parâmetros IPSec; (2) são geradas as chaves secretas necessárias; (3) o cliente descobre o endereço unicast do servidor "mais próximo"; (4) estabelece uma conexão TCP com o seu endereço unicast; (5) o cliente pede ao servidor a chave pública do grupo *Anycast*, através da conexão TCP; (6) envia ao servidor os parâmetros IPSec pretendidos para a comunicação segura, e as chaves secretas cifradas com a chave pública do grupo anycast; (7) o cliente termina a conexão TCP com o servidor, e ambos criam as SPs e SAs e introduzem estas na SPD e SAD respectivamente; (8) por último o servidor partilha com os restantes membros do grupo anycast a informação de segurança, de um modo seguro.

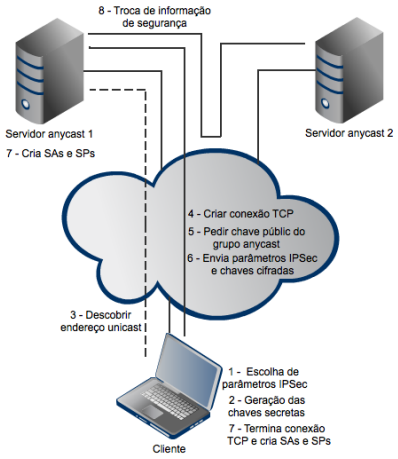

Fig. 1. Interação do cliente com o servidor

Esta solução foi concretizada com dois programas (cliente e servidor), desenvolvidos na linguagem de programação JAVA. O programa cliente deve correr na máquina cliente e o programa servidor em todos os membros do grupo *Anycast*. Estes programas utilizam o modo de configuração manual do IPSec, mas as chaves são geradas automáticamente pelo programa cliente após o utilizador escolher os parâmetros de segurança, e trocadas de um modo seguro. Utilizando criptografia assimétrica e confiando na chave pública das entidades envolvidas, garante-se que a troca de chaves secretas é feita de forma segura. Após a negociação das chaves e troca segura destas, o cliente poderá ligar-se ao serviço anycast utilizando o IPSec, independentemente do servidor para qual é encaminhado.

IV. Conclusão e trabalho futuro

Neste artigo são implementadas, testadas e avaliadas as tecnologias IPSec e anycast. Dos resultados obtidos foi possível observar que as comunicações *Anycast* não podem ser utilizadas com o IKE, podendo no entanto ser utilizadas com a configuração manual do IPSec. Desenvolveu-se um protótipo capaz de oferecer uma solução que permite a utilização do IPSec para proteger as comunicações entre um cliente e um serviço *Anycast*, tornando assim possível aliar as vantagens do IPSec e das comunicações anycast. A metodologia utilizada tem em conta o estado da arte de ambas as tecnologias, não implicando nenhuma alteração às mesmas. Esta solução permite assim, a troca segura das chaves secretas por ambas as extremidades da conexão oferecendo assim uma alternativa à utilização do IKE com o *Anycast*. Os testes efectuados permitiram verificar que o *routing*, pode ter um papel importante nos tempos de reacção a falhas.

References

[1] L. U. Scott Weber, Liang Cheng, "A survey of anycast in ipv6 networks," *EEE Communications Magazine*.

[2] K. Jun-ichiro itojun Hagino, "An analysis of ipv6 anycast," tech. rep., 2003.

[3] K. S. S. Kent, "Rfc 4301: Security architecture for the internet protocol," *Network Working Group*, 2005.